Software Engineering Institute

Maximizing Trust in the Wireless Emergency Alerts (WEA) Service

Carol Woody
Robert Ellison

February 2014

SPECIAL REPORT
CMU/SEI-2013-SR-027

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0000609

Table of Contents

Abstract **vii**

1 Introduction **1**
- 1.1 Problem Statement 1
- 1.2 Analysis of Trust Factors 1
- 1.3 Alert Originator Trust Factors 2
- 1.4 Public Trust Factors 3

2 Factors Affecting Alert Originator Trust in the WEA Service **5**
- 2.1 Appropriateness 5
- 2.2 Availability 6
- 2.3 Effectiveness 7
- 2.4 Trusting a Shared Service 8

3 Factors Affecting Public Trust in the WEA Service **9**
- 3.1 Factors to Optimize 9
- 3.2 Factors to Minimize 10
- 3.3 Maintaining Trust in a Public Service 11

4 Recommendations **12**
- 4.1 Recommendations for Alert Originators 12
- 4.2 Recommendations for FEMA and CMSPs 13
- 4.3 Recommendations for Suppliers of Emergency Management and Alerting Software 14

Appendix Trust Factor Summary Descriptions **15**

References **18**

List of Figures

Figure 1: Alert Originator Trust Factors 3

Figure 2: Public Trust Factors 4

List of Tables

Table 1:	Important Message Content Factors	9
Table 2:	Alert Originator Trust Factors	15
Table 3:	Public Trust Factors	16

Abstract

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service. Alert originators at emergency management agencies must trust WEA to deliver alerts to the public in an accurate and timely manner. Members of the public must also trust the WEA service before they will act on the alerts that they receive. Managing trust in WEA is a responsibility shared among many stakeholders who are engaged with WEA. The objective of this research was to develop recommendations for alert originators, the Federal Emergency Management Agency, commercial mobile service providers, and suppliers of message-generation software that would enhance both alert originators' trust in the WEA service and the public's trust in the alerts that it receives. To do this, researchers reviewed alerting research, interviewed alerting experts, and surveyed alert originators and the public. The researchers then identified factors that influenced trust, modeled the relationships between the trust factors using mathematical and statistical techniques, simulated and evaluated scenarios addressing various combinations of trust factor inputs on the resulting perceptions of trust, and analyzed the results to identify the most significant factors influencing trust. This report presents the recommendations that resulted from this process.

1 Introduction

1.1 Problem Statement

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS). Alert originators (AOs) at emergency management agencies (EMAs) must trust WEA to deliver alerts to the public in an accurate and timely manner. Absent this trust, AOs will not use WEA. Members of the public must also trust the WEA service. They must understand and believe the messages that they receive before they will act on them. Clearly, the AOs, the EMAs, and the Federal Emergency Management Agency (FEMA) must all strive to maximize and maintain trust in the WEA service if it is to be an effective alerting tool.

Managing trust in WEA is not the responsibility of one individual or organization. Instead, it is a responsibility of the many stakeholders who are engaged with WEA. Managing trust requires attention and action from

- the AOs to ensure that the service is used at appropriate times and that messages are correctly composed
- FEMA to ensure that the Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN) is operational and reliable
- the commercial mobile service providers (CMSPs) to ensure that their systems process WEA messages accurately and quickly
- those who supply message-generation software to the AOs to ensure that the software operates accurately, reliably, and efficiently

1.2 Analysis of Trust Factors

The objective of the Software Engineering Institute's (SEI's) research into trust in WEA was to develop recommendations for WEA stakeholders (AOs, FEMA, CMSPs, and suppliers) that would enhance both the AOs' trust in the WEA service and the public's trust in the service and the alerts received. To develop these recommendations, SEI used the following process:

1. Identify factors that influence trust through review of prior alerting research and interviews with AOs and alerting experts.
2. Survey both AOs and the public to develop an understanding of the interactions between trust factors.
3. Model the relationships between the trust factors using mathematical and statistical techniques.
4. Using these models, simulate and evaluate numerous scenarios addressing various combinations of trust factor inputs on the resulting perceptions of trust.
5. Analyze the results of the simulations to identify the most significant factors influencing trust.

This document summarizes the results of this process. For a detailed discussion of the modeling and simulation processes supporting these results, see the reports *Wireless Emergency Alerts:*

Trust Model and *Trust Model Simulations for the Wireless Emergency Alerts (WEA) Service* [Morrow 2013, Stoddard 2013].

1.3 Alert Originator Trust Factors

Many factors could influence an AO's decision to use WEA, including

- Security: the degree of confidence that the WEA service is robust against attempted cyber attacks (e.g., spoofing, tampering, and denial-of-service attacks)
- System Reliability: the degree to which AOs may depend on the WEA system to operate correctly when needed
- Public Feedback History: information received from the public regarding prior WEA messages (e.g., "thanks for warning me," "don't wake me at night")
- Historical System Feedback: information from the WEA service regarding prior performance (e.g., dissemination time, alert geolocation data)

For some factors, such as security, FEMA has requirements that an EMA and its contractors must satisfy. System reliability is a shared responsibility as it depends on the aggregate reliability of all system segments, including those that belong to the EMAs, FEMA, and CMSPs. Responding to public feedback is an AO's responsibility, but some aspects of historical system behavior such as delivery time to recipient depend on data available only from FEMA or CMSPs.

The SEI based the analysis of AOs' use of the WEA service on three key factors:

1. Appropriateness: the suitability of WEA as an alerting solution within the context of a particular incident
2. Availability: the ability of AOs to use the WEA service when needed
3. Effectiveness: the ability of the WEA service to produce the outcomes desired by AOs

These factors combine to determine WEA utilization—the decision of AOs to use the WEA service. Figure 1 shows the factors that could influence each of these system attributes. The appendix provides the factor definitions for factors affecting alert originators' trust in the WEA service. Section 2 describes the factors identified by the data analysis as significantly affecting the use of WEA.

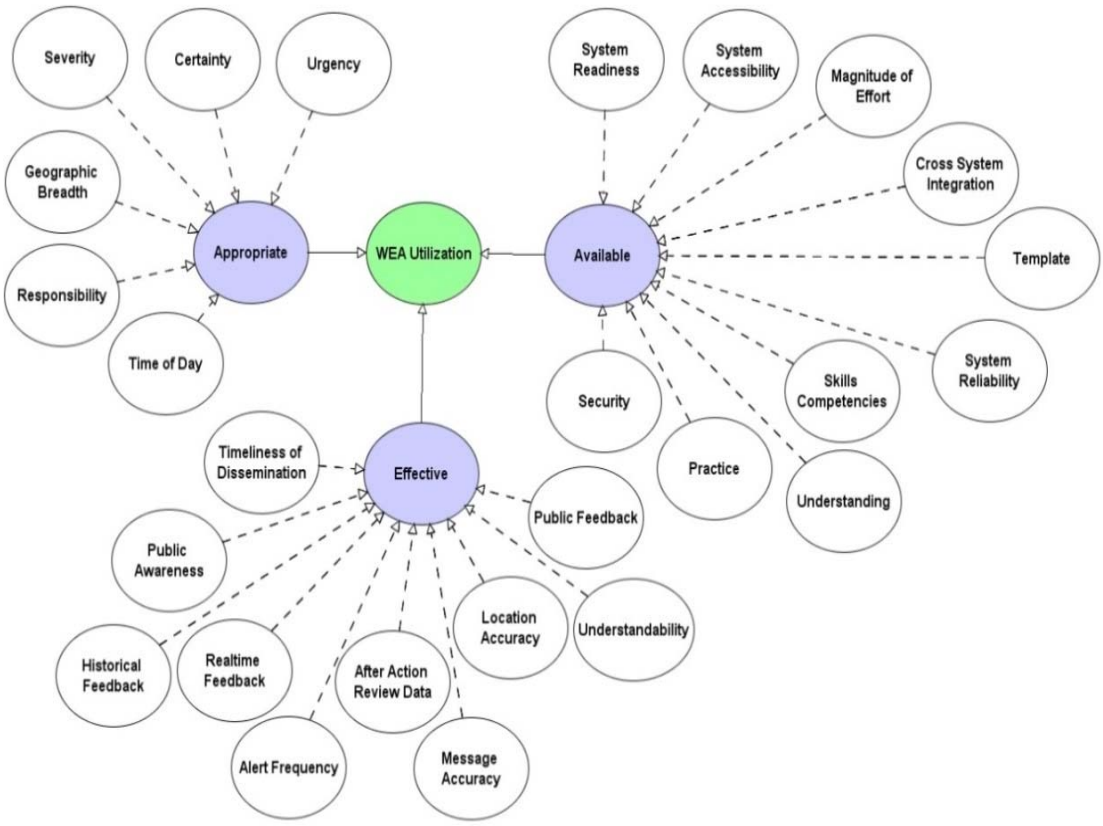

Figure 1: Alert Originator Trust Factors

1.4 Public Trust Factors

An AO should be aware of how the EMA's procedures for issuing alerts can affect public willingness to respond to those alerts. The following are some of the factors that can affect public trust in WEA:

- Public Awareness of WEA: public knowledge of WEA prior to issuance of an alert, which can be developed through outreach via media channels (television news reports, radio news reports, newspaper stories)
- Redundancy of Alerting: availability of information contained in the alert through other channels such as TV and radio, newspapers, and social media
- Lead Time Provided: the amount of time between the issuance of the alert and the moment when the public must take action
- Confirmation via Social Media: confirmation of information contained in the alert by others through social media networks such as Facebook and Twitter

The SEI analyzed the alerting service by considering a sequence of four recipient actions:

1. read or listened to an alert
2. understood the alert
3. believed that the alert was credible
4. acted on the alert

Figure 2 shows the factors that the SEI considered for each of these actions. The appendix provides the factor definitions for factors affecting public trust in the WEA service. Section 3 describes the factors identified by the data analysis as influencing desired recipient actions.

For example, an alert that concisely identifies those affected by it enables a recipient to immediately determine its relevance and should lead that recipient to act on the alert. Some factors can have both positive and negative effects. A recipient receiving redundant WEA messages via phone might consider them as spam, but redundancy via multiple channels such as radio and television would confirm the credibility of the alert. Section 3 identifies public trust factors that AOs should consider.

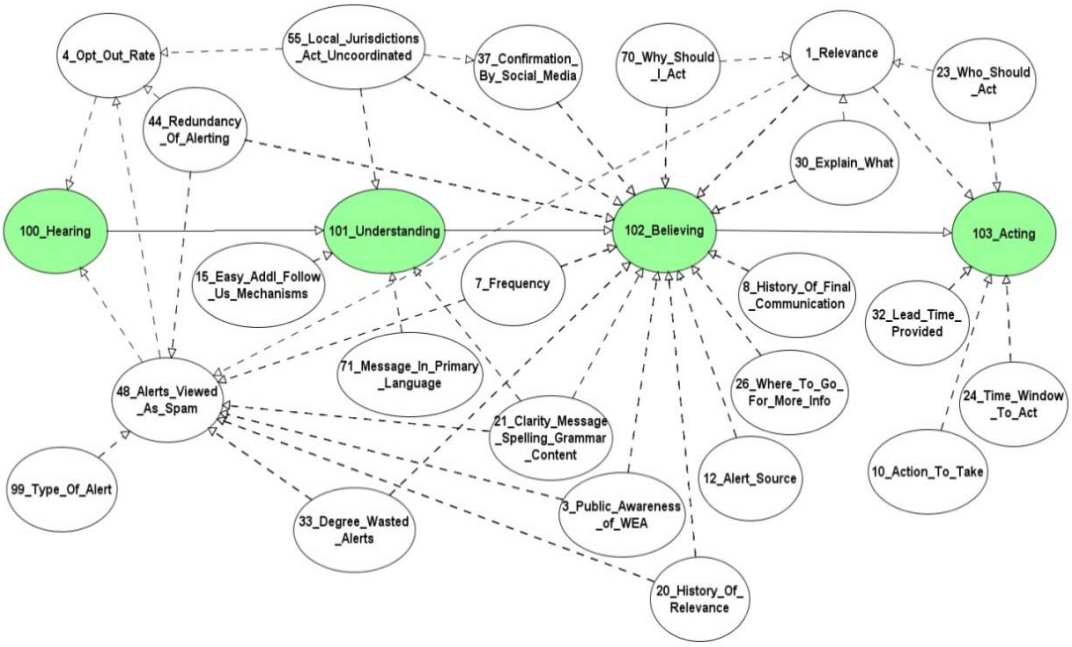

Figure 2: Public Trust Factors

2 Factors Affecting Alert Originator Trust in the WEA Service

The ultimate measure of AOs' trust in the WEA service is whether or not they use it. Based on an analysis of the AO trust model, maximizing AOs' use of the WEA service requires maximizing three key outcomes: appropriateness, availability, and effectiveness. Many factors influence each of these key outcomes, but the data from this study indicate a few that are particularly important. Because WEA is a shared service, AOs cannot control all aspects of these important factors. All WEA participants should seek opportunities for collaboration to bolster AOs' trust.

2.1 Appropriateness

Severity and Urgency

WEA is intended for use only in the most serious emergency events. The severity of the incident must be classified as either extreme or severe, posing an extraordinary or significant threat to life or property. The urgency of the incident must be classified as either immediate or expected, requiring action immediately or within the next hour. The trust model confirms the importance of these constraints. Messages issued by AOs must pertain to imminent issues that have a high impact and require prompt attention. Since this type of alert is typically infrequent, EMAs should have clear AO approval and WEA usage procedures in place to make appropriate use of WEA. In some cases, AOs may access the WEA service through integrated alerting software that issues notifications through WEA and other channels (e.g., the Emergency Alert System, Twitter, and Reverse 911). For some incidents, alerting via some of these other channels may be appropriate, while alerting through WEA is not. In these cases, the integrated software must enable AOs to determine independently when a WEA message is appropriate.

Certainty

WEA is intended for use only for incidents with a high degree of certainty. The certainty of the incident must be classified as either observed (determined to have occurred or to be ongoing) or likely (a probability of occurrence greater than 50%). Again, the trust model confirms the importance of this constraint. Alerts to be issued using WEA need to be verifiable. The AO will need information from reliable sources to confirm the immediacy of the event in order to issue a WEA message. It is important that sources provide information with sufficient timeliness for the AO to make use of WEA.

Geographic Breadth

AOs will use WEA if alerts can be targeted to the size and location of the geographic region impacted by the emergency event. The current county designations are effective in some cases, but not all. For some states, counties are huge, and notifications for an emergency in the far corner of a county send useless information to many who are hundreds of miles away and can be annoyed by the intrusion. In major metropolitan areas where the distances are smaller but population density is higher, current WEA geographic granularity may result in many people's receiving alerts for a localized event that is not relevant to them. Section 3 details how continued receipt of these irrelevant alerts desensitizes the public to the alerting process, increases the likelihood that recipi-

ents will opt out of receiving future alerts, and reduces the overall likelihood that they will receive and respond to future alerts that are indeed relevant to them.

2.2 Availability

Security

Security of the WEA system is a factor shown by the AO trust model to be important to the availability of WEA. Threats to security can exist within alert-generation technology (hardware, systems, and software), insecure integration of the WEA capability with other EMA systems, poor operational security practices, and user computing activities. An EMA, or external security experts that the EMA engages, should perform risk assessments periodically to ensure that the alerting capability is adequately secure. EMAs should conduct these risk assessments annually.

In signing the Memorandum of Agreement for access to IPAWS-OPEN and the WEA capability, an EMA agrees to meet a set of security responsibilities specified by FEMA. By implementing these security controls, AOs will protect their alert-generating systems from misuse. A compromised alert-generating system could overload the IPAWS-OPEN message validation and verification capability and delay processing of legitimate input. In addition, FEMA assigns each EMA an electronic certificate that identifies the sender of an alert to IPAWS-OPEN and authenticates each submission. Protecting the certificate so that only properly authorized messages are sent to FEMA for distribution to CMSPs is an important responsibility of each AO. Trust in WEA would diminish if an unauthorized person could send inaccurate and inappropriate WEA messages using a stolen certificate.

Many EMAs will purchase alert-generating products and services instead of building their own. AOs must ensure through their vendor selection and contracting processes that the chosen products fulfill the security responsibilities. For many products, the vendor controls the software that creates the messages for submission to IPAWS-OPEN. In this case, an EMA must give its electronic certificate to the vendor so that IPAWS-OPEN will recognize the message as legitimate. The EMA must transfer its certificate securely to the vendor and ensure that the vendor has proper protections in place to keep the certificates secure.

System Accessibility

The AO trust model identified system accessibility as a critical factor for AOs' trust. Accessibility is reduced if WEA is accessible only from a few dedicated terminals within the AOs' offices. Due to the infrequency of WEA message issuance, familiarity with the operation of these terminals will be limited, potentially resulting in delays and inaccuracies in alert issuance. Accessibility improves if AOs can access the WEA service through integration with other alerting and emergency management applications that they use more frequently. In our discussions with AOs, many of them expressed a desire for even greater accessibility, such as accessing the WEA service remotely from the scene of an incident. Although we are currently unaware of any alerting software that supports this type of remote access, it is a feature that may warrant investigation by suppliers of alerting software. Because security is also important and remote access to system capabilities can provide opportunities to an attacker as well as a legitimate user, system access must be constructed to ensure that security is appropriately maintained with increased accessibility.

For vendor-provided alerting solutions, AOs must ensure through their vendor selection and contracting processes that the chosen solution provides sufficient system accessibility with appropriate security controls.

System Reliability

In order to trust WEA, the AO must know that the system will operate reliably and transmit WEA messages successfully. Since WEA messages are expected to be infrequent, trust based on system reliability should be established through testing and not actual system use. AOs will need to confirm the reliability of the alert-generation system and the connection to IPAWS-OPEN that are under the EMA's control. AOs will also need to establish trust in the operational reliability of IPAWS-OPEN and the connections through IPAWS-OPEN to CMSPs, which are not under the EMA's control.

If the AO uses vendor-provided solutions, mechanisms for the vendor to ensure the reliability of the alert-generation capability and connections to IPAWS-OPEN should be one of the considerations in vendor selection, contracting, and performance monitoring.

AOs should also consider periodic testing of the processes that they use in issuing an alert. At a minimum, such testing should address the decision process for alert issuance, the approval process for alert issuance, and the alert creation process.

Cross-System Integration

Many EMAs handle complex alerting mechanisms that include interfaces with television and radio broadcasting, highway signage, and telephone capabilities such as Reverse 911. Cross-system integration such that WEA becomes an integral part of the operational environment will increase AOs' trust and use. Many suppliers of emergency management and alerting software products will add WEA capability to their products to provide seamless integration for their AO customers. Not all alerts will justify WEA use. Therefore, the EMA will need to structure its processes, procedures, and system capabilities so that they have mechanisms in place to take advantage of the WEA distribution channel appropriately.

2.3 Effectiveness

Timeliness of Dissemination

Timeliness of the message receipt ranked high in trust considerations. The AOs control only part of the overall message flow to the recipient but must ensure that their actions and systems do not impede the flow. The approval process for using WEA cannot not be so cumbersome and time consuming that it delays message submission. Error handling and recovery when IPAWS-OPEN rejects messages must be well-integrated parts of the message flow so problems are identified and addressed quickly. FEMA could support the AOs' measure of timeliness by providing IPAWS-OPEN distribution information periodically to each EMA for its message submissions.

Message Accuracy

AOs will use WEA if they trust its ability to disseminate correct alert information to the intended audience. The ability to structure a correct message and accurately establish a target audience for message dissemination is very important to AOs' use of WEA. AOs can select a structure of flag

settings for message content (Urgency, Severity, Certainty, Event Code, Expiration, and Response Type), and IPAWS-OPEN will generate the actual message (default mode). If an EMA chooses this mode, AOs need to review these options to ensure that they can appropriately generate the alerts that they would send through WEA from the available choices. EMAs can also choose to issue messages as text strings that IPAWS-OPEN sends to CMSPs unchanged.

Vendor software may handle message content choices for the AO. Mechanisms for the vendor to ensure message accuracy from its alert-generation capability, accuracy of recipient selection, and accuracy in structuring this information for dissemination through IPAWS-OPEN should be part of the consideration in vendor selection, contracting, and performance monitoring.

FEMA could support the AOs and build trust by providing IPAWS-OPEN feedback to each EMA about message distribution. The CMSPs could increase AOs' trust in WEA message accuracy through increased transparency about message distribution.

Historical Feedback

Knowledge gained from after-action review and analysis of each WEA usage will contribute to trust through the assembly of a track record of effective use. AOs need both public feedback and system feedback to substantiate the use of WEA over time. Trust is enhanced by feedback showing that messages are received in a timely manner and properly understood. When a vendor controls the submission capability, the AO should require the vendor to provide history information to build trust in its products and services as well as in WEA. The AO should include this feedback requirement in the contract to ensure vendor responsiveness.

2.4 Trusting a Shared Service

In addition to optimizing the factors discussed previously, AOs must also remember that WEA is a service shared by many EMAs across the country. Problems or misuse of the service by a few can impact the trust of all. Evaluation criteria for success and mechanisms for identifying and correcting problems need to be in place from the start to build AOs' trust that the system can meet their needs. Current information sharing is fragmented, and this limitation of transparency to the AO will impact trust. FEMA has assigned approval of EMAs to each state, but states do not control America's Missing: Broadcast Emergency Response (AMBER) and weather alerts, which make up the majority of use. A governing board with participants that include representatives from state EMAs as well as FEMA, the National Weather Service, the National Center for Missing & Exploited Children, and CMSPs should be considered to formalize the long-term control and monitoring of WEA and provide an effective means of information sharing among the many WEA participants.

3 Factors Affecting Public Trust in the WEA Service

The public trust was analyzed by considering the factors that could affect the following responses of a recipient:

- reading or listening to an alert
- understanding an alert
- believing an alert is credible
- acting appropriately on an alert

A recipient could read and understand an alert and then appropriately ignore it if it was not applicable. The desired outcome for the WEA service is that recipients affected by an alert take appropriate actions. The factors of most importance to AOs are those that, when present in an alert, increase the likelihood that affected recipients will act and, when absent in an alert, increase the likelihood that affected recipients will ignore the alert.

3.1 Factors to Optimize

Some factors increase public trust in the alerting service and hence increase the likelihood that recipients will act on applicable alerts. AOs should optimize these factors as much as possible. The analysis of the simulations performed for this study showed that the factors in Table 1 encouraged recipients to respond appropriately.

Table 1: Important Message Content Factors

Factor	Description	Comments
Clarity of message spelling and grammar	The degree to which an alert is free of grammar and spelling errors.	Poor grammar and spelling can lead a recipient to treat an alert as spam.
Explanation of why I should act	A justification for the action stated in the alert	The explanation provided must follow constraints limiting message size to 90 characters. A follow-up alert providing more information or a referral to a source of additional information in the first alert may be necessary. The surveys showed that it was not enough to tell people to stay indoors during a hazardous-materials event. The response was much better if an alert told them to stay indoors "to avoid chemical exposure."
Action to take	A definitive statement of action that recipients should take	
Message in primary language	Alert is provided in the primary language of the receiver	Even if respondents understood the language of the alert, if that language was not their primary language, response was reduced.

The message content was a key factor determining the trustworthiness of the message. Factors of particular importance included

- a message devoid of grammar and spelling errors
- an explanation of why that action should be taken
- a clear statement of the action that the recipient should take
- a message in the primary language of the recipient

The SEI analysis showed that the message has to be well written such that it clearly expresses the individuals affected, the reason for an action, and the recommended response. A message written in a recipient's primary language increases the likelihood that it will satisfy those message criteria.

Selected factors can be important for a specific response. SEI analysis suggested that understanding was closely coupled with recipients' ability to determine from an alert why they should act. The lead time provided by an alert also significantly affects acting. In addition, the SEI analysis showed that using multiple channels for alerts such as radio and television provided external confirmation for the credibility of an alert.

Poor composition and spelling errors could confuse a recipient, but the negative effect on message credibility and on the professionalism for an AO is equally important. There is a significant risk that poor composition and spelling errors will lead a recipient to assume that an alert is spam and ignore it.

An AO has control over message content, but the 90-character maximum size constraint affects how the message is written. That restriction increases the importance of describing how to find additional information such as including a statement about consulting local news sources. High-severity events with short lead times could require multiple alerts to provide the necessary information.

3.2 Factors to Minimize

Some factors reduce public trust in the alerting service and hence increase the likelihood that recipients will ignore applicable alerts. AOs should minimize these factors as much as possible. A number of these factors arise from operational deficiencies such as

- too many previous alerts not applicable to a recipient
- inaccurate, insufficient, or confusing information in earlier alerts
- excessive delays in delivering previous alerts
- bogus alerts following a security compromise of a WEA site

Section 2 covered these factors in detail.

Lack of coordination of alerts among local jurisdictions can increase the frequency of alerts, lead to confusion and misinformation, and raise credibility concerns for all operations. Within any jurisdiction, multiple agencies may possess authority to issue alerts. For example, within a municipality, the municipality EMA, the county EMA, the state EMA, and other state or national agencies may all have authority to issue alerts. To avoid confusion, each agency must understand which agency has the responsibility to issue an alert. This understanding is best accomplished with interagency agreements that define alerting responsibilities and regular communication among agencies. AOs must also consider interactions with neighboring jurisdictions. Since geographic distribution of WEA messages is largely influenced by cell tower location, often alerts issued in one jurisdiction will be received in neighboring ones. AOs should establish processes and communication channels with neighboring jurisdictions to notify them when an alert is being sent, enabling them to prepare for public response to the alert (i.e., calls to the 911 call center). For in-depth information on this topic, refer to the "WEA Governance Guide" in the report *Best Practices in Wireless Emergency Alerts* [McGregor 2013].

3.3 Maintaining Trust in a Public Service

Analysis of the trust factors showed that a recipient acting on an applicable alert is highly correlated with messages that are free of grammar and spelling errors, provide a justification for and a clear statement of the action to be taken, and are written in the recipient's primary language.

WEA messages are infrequently sent, and the trust that a recipient has for the WEA service could be influenced by just a few instances. While a successful alert requires that an AO give attention to multiple factors, inattention to just one factor in a single alert can reduce the credibility of the service.

With some incidents, such as fire- and weather-related events, high uncertainty leads to alerts based on the worst case. Good public awareness of WEA can help smooth issues over recipient actions that in hindsight might appear to have been unnecessary. If people have a positive image of the WEA service and understand how it works, they will be less likely to opt out of receiving WEA messages after they act on a message that proved not to affect them.

Analysis also showed that people are more likely to trust WEA if they can validate the alert information from other sources. Social media such as Twitter are good channels for distributing additional alert information about the event precipitating the WEA message. For example, such media provided information on conditions during the northeastern weather emergencies in the fall of 2012. In addition, social media services may be able to provide feedback on the public reaction to an alert, enabling EMAs to track public reaction to alert content and actual response (e.g., incident area evacuation, incident area avoidance). This feedback will help AOs handle follow-up alerts about the event and future alerts.

4 Recommendations

Combining the findings from both the AO and public trust models, we offer the following recommendations for WEA stakeholders.

4.1 Recommendations for Alert Originators

1. Use WEA only for the most urgent incidents.
2. Use WEA only for the most severe incidents.
3. Use WEA only for the most certain incidents.
4. Match geographic distribution as closely as possible to the affected area. People receiving alerts who are not impacted by the incident will consider the alerts irrelevant. Repeated irrelevant alerts will desensitize people to alerts in general and may drive them to opt out of receiving future alerts. Ensure that alerts are as focused as possible on affected areas. Weigh the benefits of alerting those impacted by an incident against the detriments of alerting those not impacted.
5. Establish a comprehensive security plan to protect both physical and electronic access to your alert-generation capability. The security plan should include the acquisition and operation of all system and software components. Plan security for outsourced services such as network management, or ensure that the supplier does. The security plan should include an annual security risk assessment because cyber threats evolve.
6. When acquiring or developing WEA message-generation software, consider software reliability, that is, the creation and transmission of messages in a timely and accurate manner. Survey responses from AOs indicated reduced willingness to use WEA as reliability declined from 99.9% to 99% to 90%.
7. If you issue WEA messages using the default method of construction, study the WEA specifications to understand the mapping between Common Alerting Protocol (CAP) inputs and the resulting WEA message. In the default mode of issuing WEA messages, IPAWS-OPEN automatically constructs the alert message as a standard combination of phrases derived from your data in the CAP fields defining Urgency, Severity, Certainty, Event Code, Expiration, and Response Type. In these cases, it is important for you to know what message will result from your inputs.
8. If you issue WEA messages using Commercial Mobile Alert Message (CMAM) text,[1] develop templates to guide the message creation process, and practice distilling alerts into 90-character messages. It is important that AOs carefully craft an understandable and accurate message. Evaluate the resulting message for accuracy, clarity, voice, grammar, and spelling.

1 Check with FEMA to determine whether your Collaborative Operating Group (COG) is authorized to use CMAM text.

9. Ensure that AOs can perform the processes to decide to issue a WEA message, to approve the issuance, and to compose and transmit the message in a time frame consistent with the alert urgency.

10. Monitor public feedback after issuing a WEA message. Hold after-action review sessions to assess the effectiveness of the alerting process and the outcome of the alerting action. Use this information to drive improvements in the alerting process.

11. Ensure that messages include clear statements of the action that recipients should take. If you use the default mode of message construction, this is automatically provided by IPAWS-OPEN. If you construct the message using CMAM text, be sure to include this information.

12. When possible, include an explanation of why the specified action is needed. This increases the likelihood that alert recipients will understand, believe, and act on the message. If you use the default mode of message construction, no mechanism is available to include this information. However, if you construct the message using CMAM text, be sure to incorporate this information.

13. Be aware of the language demographics within your alerting area. Alert recipients are more likely to respond to a message written in their primary language than in an alternative language, even if they understand that alternative language. If you use the default mode of message construction, no mechanism is available to include information in any language other than English. However, if you construct the message using CMAM text, consider issuing the alert in the language most suitable for the target population. For mixed populations, you may want to issue multiple alerts in multiple languages.

14. Coordinate your alerting activities with neighboring and overlapping jurisdictions. Within your jurisdiction, multiple agencies may have alerting authorities and responsibilities (e.g., municipal EMA, county EMA, state EMA, and NWS). You should meet with these agencies and establish clear guidelines for determining who will issue alerts. You should also establish communications channels to coordinate with surrounding jurisdictions. In many cases, alerts issued in one jurisdiction may bleed over into neighboring ones. You should notify neighboring jurisdictions when you issue an alert to enable them to propagate that alert throughout their jurisdictions, if appropriate, or to address the public response to your alert.

4.2 Recommendations for FEMA and CMSPs

1. Consider reducing the required geotargeting resolution to an area smaller than a county or FIPS code. Many CMSPs already support finer resolution; however, until all CMSPs in an area do so, AOs cannot rely on this improved resolution.

2. Ensure that IPAWS-OPEN and the WEA service operate reliably, that is, transmit messages in a timely and accurate manner. Survey responses from AOs indicated reduced willingness to use WEA as reliability declined from 99.9% to 99% to 90%.

3. Consider support of alternative languages in the alerting process. Currently, AOs who generate alerts using CMAM text can issue alerts in languages suited to the demographics of the alerted area. However, alerts generated by IPAWS-OPEN in response to AOs' CAP inputs

can only be issued in English. Enabling AOs to choose among several common languages for these messages could enhance public receptiveness and response.

4.3 Recommendations for Suppliers of Emergency Management and Alerting Software

1. Incorporate adequate security into alert-generation products. During development, reduce the risk of vulnerabilities by considering how the system and software could be compromised. Document a product's security controls and processes. In addition, all user input should always be validated. Designing the software to authenticate users and control their actions is preferable to using authentication information that other components provide. Ensure that access to sensitive data such as an IPAWS-OPEN digital certificate is securely managed.

2. Consider developing and offering a capability that enables incident field commanders to remotely access alert-generation software through secure mobile communications links. Effective integration of this capability with alert-generation product security is important to AOs' use.

3. Ensure that alert-generation software operates reliably, that is, creates and transmits messages in a timely and accurate manner. Survey responses from AOs indicated reduced willingness to use WEA as reliability declined from 99.9% to 99% to 90%.

4. Consider integrating WEA message-generation capabilities with other products that have emergency management and alert-generation capabilities. Such integration maximizes AOs' familiarization with the alert-generation process and aids AOs in maintaining necessary competencies for the infrequently used WEA capability.

5. Ensure that AOs can compose and transmit WEA messages in a time frame consistent with the alert urgency.

6. For WEA messages generated using the default method of construction (i.e., IPAWS-OPEN automatically constructs the alert message as a standard combination of phrases derived from AO data in the CAP fields defining Urgency, Severity, Certainty, Event Code, Expiration, and Response Type), ensure that your software provides feedback to AOs showing them the actual message that IPAWS-OPEN will construct in response to the CAP inputs provided.

7. For WEA messages generated using CMAM text,[2] provide the capability for AOs to use templates to guide the message creation process. Also provide tools to check message accuracy, clarity, voice, grammar, and spelling.

8. Consider supporting alternative languages in the alerting process. Currently, alerts generated by IPAWS-OPEN in response to AOs' CAP inputs can only be issued in English. However, AOs that generate alerts using CMAM text could issue these alerts in languages suited to the demographics of the alerted area. Ensure that message-generating software supports alert generation in selected alternative languages. Include tools to check message accuracy, clarity, voice, grammar, and spelling.

2 Check with FEMA to determine whether your COG is authorized to use CMAM text.

Appendix Trust Factor Summary Descriptions

Table 2: Alert Originator Trust Factors

Factor	Definition
Accuracy	The ability of the WEA system to disseminate correct alert information to intended recipients
After-action review data	Knowledge resulting from in-house review and analysis of prior WEA message dissemination
Alert frequency	The number of WEA messages issued within an area in the immediate past
Appropriateness	The degree to which WEA provides an alerting solution that is appropriate to the event
Authority	Permission and prerogative of the AO to issue the alert
Availability	The degree to which the WEA system is capable of being used when needed to issue an alert
Certainty	The verifiability of the associated event is sufficient to justify a WEA message
Cross-system integration	The ability of the WEA service to work in conjunction with other emergency management systems
Effectiveness	The degree to which the WEA service accomplishes its intended purpose
Geographic breadth	The size and location of the geographic region impacted by the emergency event is consistent with WEA capabilities
Historical system feedback	Information from the WEA service regarding prior performance (e.g., dissemination time, alert geolocation data)
Location accuracy	The ability of the WEA service to disseminate alerts to the defined locations
Magnitude of effort	The amount of time and work needed to issue the alert
Message accuracy	The ability of the WEA service to disseminate alerts with the message content intended by the AO
Message understandability	The ability to convey necessary information within the constraints of the WEA message
Practice	The exercising of skills needed to operate the WEA service effectively
Public awareness/outreach	The establishment of prior awareness and public education regarding WEA services
Public feedback history	Information received from the public regarding prior WEA messages (e.g., “thanks for warning me,” “don't wake me at night”)
Real-time system feedback	Information from the WEA service reporting the status of the current WEA message dissemination process (e.g., message delivered, message rejected)
Remote/portable access	The ability of AOs to generate WEA messages from remote locations
Responsibility	The AO's obligation and authority to issue the alert (i.e., is it clear that the responsibility and authority to issue the alert resides with the EMA, or could other organizations be responsible for issuing the alert?)
Security	The degree of confidence that the WEA service is robust against attempted cyber attacks (e.g., spoofing, tampering, and denial-of-service attacks)
Severity	The degree of impact associated with an event is consistent with WEA usage
Skills/competencies	The aptitude and capability to operate the WEA service effectively

Factor	Definition
System accessibility	The ability of AOs to gain access and admittance to the WEA service when and where desired
System ease of use	The facility (or difficulty) with which AOs may use the WEA service to issue alerts
System feedback	The quality and value of information describing system function that the WEA service provides to the AO
System readiness	The degree to which the WEA service is operable and ready for use when needed
System reliability	The degree to which AOs may depend on the WEA system to operate correctly when needed
Templates	The availability of predefined formats and information to accelerate and ease the process of alert issuance
Time of day	The time of day (e.g., waking hours, middle of the night) when the EMA will issue the alert
Timeliness	The ability of the WEA service to disseminate a WEA message within a suitable time frame
Training	Creation of skills, competencies, and knowledge for AOs
Understanding	The knowledge of the operational characteristics of the WEA service
Urgency	The degree of immediacy associated with an event is consistent with WEA usage

Table 3: Public Trust Factors

Factor	Description
Acting	Recipient takes action stated in the alert
Action to take	A definitive statement of action that recipients should take
Alert source	The governmental tier of the sender (i.e., local, county, state, federal)
Alerts viewed as spam	Alerts are prejudged as spam
Believing	Recipient accepts the alert as true
Clarity of message spelling and grammar	The degree to which an alert is free of grammar and spelling errors
Confirmation via social media	Information contained in the alert is disseminated by others through social media networks such as Facebook and Twitter
Easy additional follow-us mechanisms	Ease of obtaining additional information from the sender via other communications channels
Explanation of what has happened	A definitive statement of the event that has precipitated the alert
Explanation of why I should act	A justification for the action stated in the alert
Frequency	The time rate at which alerts are received (e.g., alerts per month)
Hearing	Recipient receives and reads the alert
History of final communication	Issuance of a final communication (e.g., all-clear notice) at the end of the event
History of relevance	The applicability of previously received alerts to the recipient
Lead time provided	The amount of time between the issuance of the alert and the moment when recipients must take action

Factor	Description
Local jurisdictions act uncoordinated	The level of cooperation between senders within a region, as evidenced by avoidance of redundant alerting, agreement between alerts, etc.
Message in primary language	Alert is provided in the primary language of the receiver
Opt-out rate	The percentage of alert receivers who choose to disable the receipt of future alerts
Public awareness of WEA	Public knowledge of WEA prior to issuance of an alert, developed through outreach via media channels (TV news reports, radio news reports, newspaper stories)
Redundancy of alerting	Information contained in the alert is also available through other channels such as TV and radio news
Relevance	Applicability of the alert to the receiver: Does it affect the receiver's current location? Is it received at the appropriate time? …
Time window to act	A definitive statement of when the recipient should take the actions stated in the alert
Type of alert	Presidential, Imminent Threat, or AMBER
Understanding	Recipient comprehends the information provided in the alert
Where to go for more information	A definitive statement of places to seek additional information regarding the event precipitating the alert
Who should act	A definitive statement of which recipients should take the actions stated in the alert

References

[McGregor 2013]

McGregor, John D.; Elm, Joseph P.; Trocki Stark, Elizabeth; Lavan, Jennifer; Creel, Rita; et al. *Best Practices in Wireless Emergency Alerts* (CMU/SEI-2013-SR-015). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70001

[Morrow 2013]

Morrow, Timothy B.; Larkin, Christopher; Stoddard, Robert W.; & Elm, Joseph P. *Trust Model Simulations for the Wireless Emergency Alerts (WEA) Service* (CMU/SEI-2013-SR-026). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70032

[Stoddard 2013]

Stoddard, Robert W.; Elm, Joseph P.; McCurley, Jim; & Sheard, Sarah. *Wireless Emergency Alerts: Trust Model* (CMU/SEI-2013-SR-021). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70115

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Maximizing Trust in the Wireless Emergency Alerts (WEA) Service	FA8721-05-C-0003

6. AUTHOR(S)

Carol Woody and Robert Ellison

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

CMU/SEI-2013-SR-027

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Trust is a key factor in the effectiveness of the Wireless Emergency Alerts (WEA) service. Alert originators at emergency management agencies must trust WEA to deliver alerts to the public in an accurate and timely manner. Members of the public must also trust the WEA service before they will act on the alerts that they receive. Managing trust in WEA is a responsibility shared among many stakeholders who are engaged with WEA. The objective of this research was to develop recommendations for alert originators, the Federal Emergency Management Agency, commercial mobile service providers, and suppliers of message-generation software that would enhance both alert originators' trust in the WEA service and the public's trust in the alerts that it receives. To do this, researchers reviewed alerting research, interviewed alerting experts, and surveyed alert originators and the public. The researchers then identified factors that influenced trust, modeled the relationships between the trust factors using mathematical and statistical techniques, simulated and evaluated scenarios addressing various combinations of trust factor inputs on the resulting perceptions of trust, and analyzed the results to identify the most significant factors influencing trust. This report presents the recommendations that resulted from this process.

14. SUBJECT TERMS	15. NUMBER OF PAGES
emergency alerting, trust factors, trust model, Wireless Emergency Alerts	29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102